IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Messaoud Benantar		
Assignee:	International Business Machines Corporation		
Title:	Method and System for Computing Digital Certificate Trust Paths Using Transitive Closures		
Serial No.:	10/045,112	Filing Date:	January 10, 2002
Examiner:	Shin Hon Chen	Group Art Unit:	2131
Docket No.:	AUS920010943US1	Customer No.	65362

December 12, 2008

FILED ELECTRONICALLY

SUPPLEMENTAL APPEAL BRIEF SUBMISSION UNDER MPEP § 1205.03

Dear Sir:

In response to the Notification of Non-Compliant Appeal Brief dated November 13, 2008, Applicant files this Supplemental Appeal Brief Submission pursuant to MPEP § 1205.03 for purposes of identifying and separately referring each independent claim to the specification by page and line number. It is believed that no fee is due in connection with this Supplemental Appeal Brief, however, the Board is authorized to deduct any amounts required for this supplemental appeal brief and to credit any amounts overpaid to Deposit Account No. 090447.

As a preliminary matter, Applicant respectfully submits that the original Appeal Brief fully meets the requirements of 37 C.F.R. § 41.37(c)(1)(v), and that there is no requirement in the patent rules that a concise explanation (with corresponding page and line number) be "separately" provided for each independent claim. To the contrary, all that is required by 37 C.F.R. § 41.37(c)(1)(v) is a "concise explanation of the subject matter defined in each of the independent claims involved in the appeal, which shall refer to the specification by page and line number, and to the drawing, if any, by reference characters." While the objection appears to exalt form over substance, Applicant submits this supplemental appeal brief submission solely for purposes of expediting consideration of the appeal to separately refer each independent claim involved in the appeal to the specification by page and line number, and to the drawing, if any, by reference characters.

V. SUMMARY OF CLAIMED SUBJECT MATTER - 37 CFR § 41.37(c)(1)(v)

The claims of the present patent application are directed to a method, system, apparatus, and computer program product are presented for managing digital certificates. When entities need to engage in a secure transaction or open a secure communication link, they may exchange digital certificates in order to provide a public key or reference information to a public key for the opposing entity, thereby requiring validation of a received certificate. Rather than construct a trust path for each validation event, hierarchical certifications and peer-to-peer cross-certifications among a set of certificate authorities are represented by a set of trust relations, and trust path information is generated using a "transitive closure computation" and an "all pairs shortest paths" computation over the set of trust relations and then incrementally updated as the set of trust relations changes. Computations related to trust paths can be delegated to a central agent in a trust web.

The subject matter defined in independent claim 1 may be understood with reference to the example embodiments depicted in Figures 4 and 5 which depict a method, apparatus and computer program product for processing digital certificates within a data processing system. Referring now to Figure 4, the method begins at step 402 when a set of trust relations are determined between a set of certificate authorities (CAs) in a trust web. At step 404, the set of trust relations are represented in an adjacency matrix in which each cell in the adjacency matrix corresponds to a pair of certificate authorities. At step 406 (and Figure 5), a "transitive closure computation" is performed on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities. And at step 410, a separate "all-pairs-shortest-paths" computation is performed on the adjacency matrix to generate multiple sets of shortest trust paths between the certificate authorities. *See, e.g.*, Application, Figures 4, 5A-B, and ¶¶ 12, 28-32, 67-86 (page 5, lines 1-21; page 9, line 24 to page 11, line 28; and page 25, line 3 to page 33, line 14). The subject matter defined in independent

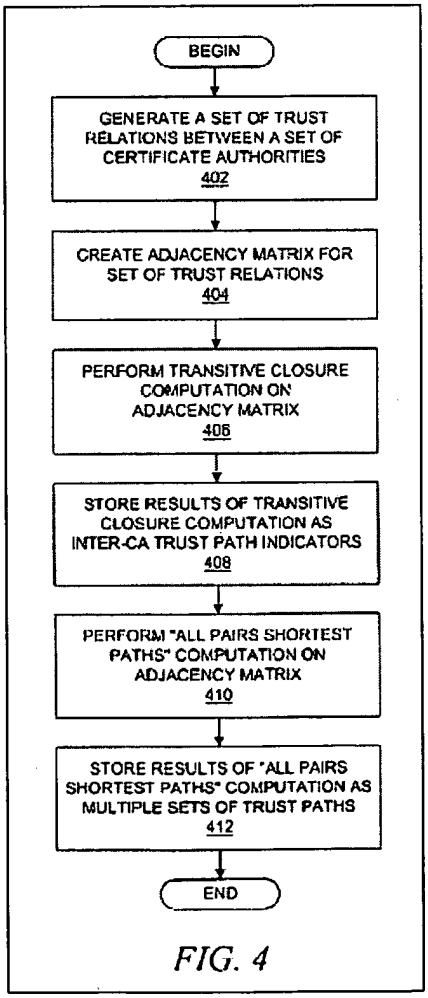

FIG. 4

claim 4 may also be understood with reference to the example embodiments depicted in Figures 4-5 and the associated description in the Application at page 5, lines 1-21; page 9, line 24 to page 11, line 28; and page 25, line 3 to page 33, line 14. In addition, the subject matter defined in independent claim 7 may be understood with reference to the example embodiments depicted in Figures 4-5 and the associated description in the Application at page 5, lines 1-21; page 9, line 24 to page 11, line 28; and page 25, line 3 to page 33, line 14.

The subject matter defined in independent claim 10 may be understood with reference to the example embodiments depicted in Figures 6 and 8B-C which depict a method, apparatus and computer program product for operating certificate authorities within a data processing system. Referring now to Figure 8B, the method begins at step 822 when a trust relation with a second certificate authority is established at a first certificate authority (CA). At step 824, a trust relation update message is sent to a central trust web agent which processes the trust relation information for a set of certificate authorities within a trust web. *See, e.g.*, Application, Figures 6, 8B-C, and ¶¶ 12, 28-32, 87-88 and 94-98 (page 5, lines 1-21; page 9, line 24 to page 11, line 28; page 33, line 15 to page 34, line 11; and page 36, line 4 to page 38, line 18). The subject matter defined in independent claim 14 may also be understood with reference to the example embodiments depicted in Figures 6, 8B-C and the associated description in the Application at page 5, lines 1-21; page 9, line 24 to page 11, line 28; page 33, line 15 to page 34, line 11; and page 36, line 4 to page 38, line 18. In addition, the subject matter defined in independent claim 18 may be understood with reference to the example embodiments depicted in Figures 6, 8B-C and the associated description in the Application at page 5, lines 1-21; page 9, line 24 to page 11, line 28; page 33, line 15 to page 34, line 11; and page 36, line 4 to page 38, line 18.

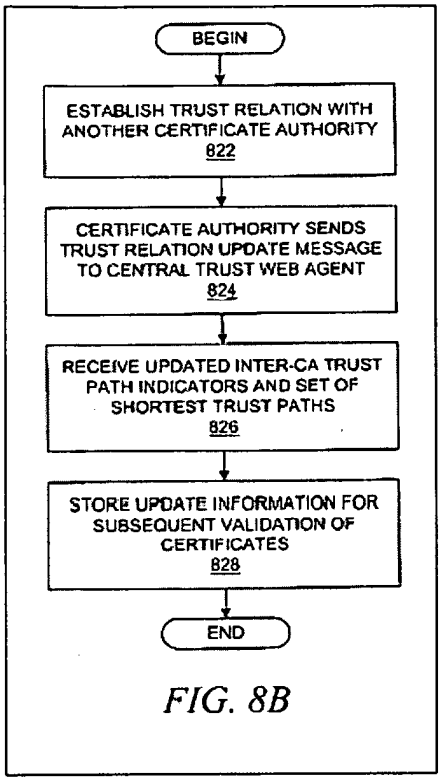

FIG. 8B

Finally, the subject matter defined in independent claim 22 may be understood with reference to the example embodiments depicted in Figures 6 and 8B-C which depict a method, apparatus and computer program product for operating certificate authorities within a data

processing system. Referring now to Figure 8C, the method begins at step 832 where a central trust web agent receives a trust relation update message from a certificate authority (CA) and processes the trust relation information for a set of certificate authorities within a trust web, where the trust relation update message indicates a change in a set of trust relations for the certificate authority. At step 834, a set of trust relations for the set of certificate authorities within the trust web is modified based on an indicated request in the trust relation update message. *See, e.g.*, Application, Figures 6, 8B-C, and ¶¶ 12, 28-32, 87-88 and 94-98 (page 5, lines 1-21; page 9, line 24 to page 11, line 28; page 33, line 15 to page 34, line 11; and page 36, line 4 to page 38, line 18). The subject matter defined in independent claim 25 may also be understood with reference to the example embodiments depicted in Figures 6, 8B-C and the associated description in the Application at page 5, lines 1-21; page 9, line 24 to page 11, line 28; page 33, line 15 to page 34, line 11; and page 36, line 4 to page 38, line 18. In addition, the subject matter defined in independent claim 28 may be understood with reference to the example embodiments depicted in Figures 6, 8B-C and the associated description in the Application at page 5, lines 1-21; page 9, line 24 to page 11, line 28; page 33, line 15 to page 34, line 11; and page 36, line 4 to page 38, line 18.

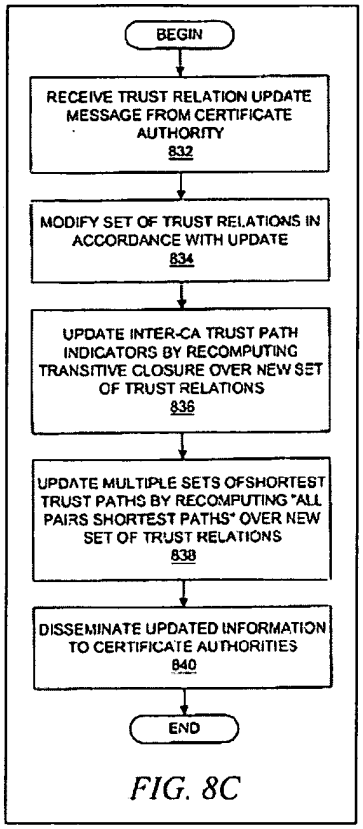

FIG. 8C

As seen from the foregoing, the subject matter of the independent claims is set forth in the Application at Figures 1A-B, 4, 5A-5B, 6-7, and 8A-8C and the associated description, including ¶¶ 12, 13-15, 18-32, and 66-98 (page 5, lines 1-12; page 6, lines 1-15; page 6, line 21 to page 11, line 28; page 25, line 3 to page 38, line 18), though additional contextual description is provided in the application and claims section. While Applicant has identified passages from the specification to explain the independent claim subject matter and how it may be implemented with a computer program product or apparatus for processing certificates within a data processing system, it will be appreciated that the referenced description includes contextual information to provide an overall context for an example embodiments, and therefore should not be used to improperly read limitations from the specification into the claims.

CONCLUSION

In view of the above second supplemental description providing a summary of the claimed subject matter, Applicants request that the Notification of Non-Compliant Appeal Brief be withdrawn and that the pending rejections of the claims should not be sustained.

CERTIFICATE OF TRANSMISSION

I hereby certify that on December 12, 2008, this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Michael Rocco Cannatti/

Respectfully submitted,

/Michael Rocco Cannatti/

Michael Rocco Cannatti
Attorney for Applicant(s)
Reg. No. 34,791